The HIPAA Implementation Newsletter
Issue #52 – Friday, February 28, 2003
| Security | Litigation | States | Insurance |
Web format with links at http://lpf.com/hipaa/

3rd Year

Issue number one of The HIPAA Implementation Newsletter was published on March 2, 2001. This issue begins our third year of publication. Thank you for your continuing interest and support and for passing it along to your friends and colleges.

DWT Analysis & Comments on Security Rules

"…After the 60-day period mandated by the Congressional Review Act and 24 months mandated by the HIPAA statute, the security rules will become effective for enforcement purposes in April 2005. … The 2005 effective date tells only part of the story. The "mini-security rule" in the HIPAA privacy rules (45 CFR 164.530(c)) goes into effect in less than two months. It requires covered entities and their business associates, as of April 14, 2003, to implement "appropriate administrative, technical and physical safeguards" for protected health information in all forms, non-electronic and electronic. It is likely that the meaning of "appropriate safeguards" under the privacy rules will in part be determined by referring to the … new final security rules. Viewed in this perspective, the first impact of the new security rules is almost immediate.

"The document released by HHS contains the rules and a long explanatory preamble. For those of you who need to read the entire document, we suggest that you go first to the back, to page 245, and start with the rules themselves (45 typed pages). Then go back to the beginning of the document to read the 244-page preamble. Things will fall into place faster. …

"… The new rules discard much of the proposed security rules' terminology in favor of definitions in common with the privacy rules. For example, the requirements of a "chain of trust" agreement in the proposed security rules are now additional "business associate" contract requirements.

"Generally speaking, the final security rules offer less detail and more generic guidance, in the sense of high-level direction, about how covered entities and their business associates should go about implementing security. As HHS says, "we have focused more on what needs to be done and less on how it should be accomplished."

"This means that the new rules are less a series of checklists and more a description of principles for each covered entity and business associate to evaluate and apply, based on the entity's specific situation. One benefit to this approach, as a general matter, is less regulatory risk through the enforcement process. Other risks remain however, because of the new rules' demands on covered entities to exercise constant vigilance and apply prudent judgment about security to changing circumstances. These are familiar litigation risk management issues.

"The new security rules' scope is narrowed to protected health information (PHI) in electronic form only. Consequently, many details of implementing the security rules may not apply to PHI that is not in electronic form. However, HHS emphasizes that the privacy rules apply to PHI in any form. … It requires that "appropriate" security be applied to all PHI in any event, whether or not the security rules themselves apply.

"One area of vast improvement is the final security rules' explicit recognition that the cost of implementing security is a factor in security decisions (and, presumably, in regulatory and judicial judgments about security issues). The entire health care industry benefits from this dose of realism ... At the same time, HHS cautions that cost considerations do not justify ineffective security. "[T]here is a clear requirement that adequate security measures be implemented . . . . Cost is not meant to free covered entities from this responsibility."… While this approach does not eliminate all enforcement or litigation risk, it improves the regulatory climate substantially.

"The new rules have "standards" and "implementation specifications." Implementation specifications can be either "required" ("R") or "addressable" ("A"). Appendix A to the rules is a "Security Standards Matrix" that lists each standard and its associated implementation specifications. The matrix shows by an "R" or "A" whether the particular implementation specification is required or addressable, and lists the section of the security rules where the standard and implementation specification are found.

"Essentially, a standard explains what must be done, and implementation specifications explain how to do it. If HHS believes that an implementation specification is one of many options, none of which by itself is essential, then it will label the implementation specification "addressable" ("A"). If HHS sees the implementation specification as essential, it will be "required" ("R").

"The standards are grouped under three headings: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. While there remains inevitable overlap, these categories prove more streamlined than the organization of the proposed security rules.

"HHS instructs that the place to start thinking about security under the new rules is section 164.306. This section is the heart of the new security rules, and tracks the part of the HIPAA statute that governs security standards and safeguards. Covered entities must meet four security requirements …:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance . . . by its workforce.

"Section 164.306(b) specifically calls for a flexible approach: "Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." The rules allow covered entities to

factor in cost, size, complexity, technical infrastructure, other capabilities, and the likelihood and seriousness ("criticality") of potential security risks. …
"However, there is significant flexibility in approach because so many of the implementation specifications are addressable, not required. A covered entity must assess whether each addressable specification is reasonable and appropriate for its unique situation. Then it has choices. If the specification is reasonable and appropriate for that covered entity, it "must" be implemented. If it is not reasonable and appropriate, the entity must either implement another equivalent measure that is reasonable and appropriate or, if the standard can be met some other way, choose not to implement the specification or any equivalent specification. **The covered entity must document the reasons for its choice.**
"… The first step is to assess the security risks it faces. Then it must implement countermeasures proportional to those risks, and manage its countermeasures to keep up with new or increased risks. ... By the way it has written section 164.306 and explained it in the preamble, HHS has set a high standard for security, and narrowed legal arguments about how to interpret the HIPAA statute's language about safeguards.
"HHS refers several times to guides published by NIST, the National Institute of Standards and Technology, as an aid in risk assessment and in the security management process. …The guides will also be important references in HHS's enforcement of the security rules and in other litigation over security issues. …
"… the new security rules only set out a process for decision-making. They do not make the decisions nor prescribe any particular technology. Indeed, the preamble is determinedly and explicitly technology-neutral. …
"The new rules require covered entities and business associates to manage security processes assiduously. There is new emphasis, for example, on an entity's ability to detect an intrusion (such as a hacker attack) and respond quickly and effectively with countermeasures. This is known as "incident response." …
"… whether security countermeasures are good enough to "ensure" the confidentiality, integrity, and availability of PHI, and protect it from "any" hazard one could reasonably anticipate, is likely to be judged retroactively. Results and the documentation of decisions will both be important. … there is inherent exposure to legal liability. It cannot be eliminated, and the new rules do not attempt to do so.
"[The final rules] require covered entities to have agreements with business associates who create, receive, maintain or transmit electronic protected health information on the covered entity's behalf. These agreements must contain assurances from the business associate that it will appropriately safeguard the information.
+ More at: http://www.dwt.com/practc/hc_ecom/bulletins/02-03_HIPAASecRules.htm

Security Rules and Litigation

"Richard Marks, a lawyer at the Seattle-based law firm of Davis Wright Tremaine LLP, said the combination of the privacy rules and the long-delayed and open-to-interpretation security standards could become a honey pot for law firms that specialize in class-action suits. Those firms, Marks said, believe HIPAA could be as lucrative as "asbestos and breast implant litigation combined." Asbestos and breast implant lawsuits in recent years have resulted in costly settlements and bankrupted companies in both fields. …
"Marne Gordon, director of regulatory affairs at TruSecure Corp. in Herndon, Va., agreed. "This is all headed for the courts. Everyone is looking to establish case law." Gordon said she is also concerned that litigation-shy health care organizations may stick with paper records rather than roll out computerized physician order entry systems that could save lives by eliminating medical errors caused by paper records (see story).
"… CMS dropped many mandated requirements contained in an earlier proposed rule, making them merely "addressable," Trudel said. In other words, they're optional. For example, the encryption of PHI transmitted over the Internet is no longer mandated and can be based on risk assessment. That means that when one doctor sends e-mail to another doctor about a patient consultation, encryption may not be necessary. But if "you're a large [health care] organization sending a bunch of transactions, then you would want to encrypt," Trudel said.
"Jeff Fusile, a consultant at PricewaterhouseCoopers, disagreed, saying that in his view a doctor-to-doctor e-mail of a consultation on a patient with an AIDS diagnosis would definitely require encryption under the HIPAA security standards. That shows how risk analysis is key to implementing a security standard that doesn't mandate policies, procedures or technologies but requires health care organization instead "to think about and determine what is reasonable," Fusile said.
+ More at:
http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,78684,00.html

Privacy Litigation

"The D.C. Superior Court recently found the Washington Hospital Center guilty of disclosing one patient's protected health information (PHI) to coworkers. John Doe … was awarded $250,000 for damages relating to breach of confidential relationship after the receptionist revealed the man's HIV positive status to his coworkers. Doe claimed that … the Center was in breach of confidential relationship by … allowing the receptionist access to PHI.
+ More at:
http://www.thompson.com/hp_newsbriefs/030220a_healthcare.html
"An employee at Abbott Northwestern Hospital, Minneapolis, and an employee at Park Nicollet Clinic, St. Louis Park, allegedly stole Social Security numbers from several former patients to open fraudulent credit card and phone accounts. … eight people had been charged in the identity theft crime

ring. …The group … allegedly ran up purchases of more than $78,000.
More at: http://www.mnsun.com/story.asp?city=Bloomington&story=108288
"An investigation is underway after medical test results from an Ottawa clinic ended up on the back of real estate flyers delivered to Toronto homes. One flyer shows pictures of houses for sale on one side, and the results of a mammogram done at the Ottawa Hospital on the other. … an investigation has found the woman's records were released … to a Toronto law office. "If it does turn out to be from a law office, I would be very concerned how widespread confidential information gets. I would think a law office would be up to date on confidentiality and security issues," … patient-confidentiality rules prevented him from identifying the law firm.
More at:
http://ottawa.cbc.ca/template/servlet/View?filename=ot_privacy20030220

HIPAA and States

"With state budgets suddenly tight, this year's HIPAA deadlines are an unwelcome guest. … With two HIPAA deadlines in 2003 and no money to meet them, "there's going to be fewer states done on time, and more shortcuts taken," says Wes Rishel, vice president and research area director for the Gartner Group, Stamford, Conn. … One estimate puts the total price tag for state and local compliance at $3.5 billion, rivaling the costs of Y2K compliance.
"Local governments--mostly counties, which administer many programs--tend to be less prepared. "The counties and the municipalities are in dismal shape for the most part," Rishel says. "I talked to a county official in Wisconsin who said, 'I'm selling snowplows to make payroll. How am I going to pay for HIPAA?' "
"States with a central office overseeing all HIPAA compliance activities--such as California, North Carolina and Ohio--are in better shape. But even North Carolina's model program has been slashed from 12 employees to five because of budget cuts. The cuts have prompted a bare-bones approach to writing basic privacy policies, says Sarah Brooks, manager of the state's HIPAA office. "It's doubtful we'll have everything in place for April," Brooks says.
+ More at:
http://www.hospitalconnect.com/hhnmag/jsp/articledisplay.jsp?dcrpath=AHA/NewsStory_Article/data/0302HHN_InBox_HIPAA&domain=HHNMAG

Hacking-related Insurance Costs Soar

"Computer worms and viruses cost companies time and cleanup costs — and now higher insurance premiums. Many insurance companies … have sliced hacking losses from general-liability policies, forcing companies to spend extra for "network risk insurance," which costs about $5,000 to $30,000 a year for $1 million in coverage.…That's a dangerous proposition. Losses from computer crime are expected to soar 25% to $2.8 billion in the USA this year, says market researcher TruSecure. Successful Web-site attacks nearly

doubled to 600 a day. Hacker insurance is expected to jump from a $100 million market today to $900 million by 2005, market researcher Gartner says.

"Hacker insurance will be ubiquitous in a few years," says Bruce Schneier, chief technology officer of Counterpane Internet Security. "You can't budget for the next computer worm, but insurance is a fixed cost that reduces risk."…In addition to the premium, companies have to pay upfront to have their networks assessed. That can cost thousands. And hacker insurance isn't entirely foolproof, security experts warn. Some coverage is limited and may not cover sophisticated worms and viruses that have yet to surface.
+More at: http://www.usatoday.com/tech/news/computersecurity/2003-02-09-hacker_x.htm

Conferences and Webinars

On July 2, last year, almost 500 people joined us on a Webinar hosted by Search Security. [Issue 38] We have been invited to take another look at HIPAA and will be presenting **'Where Are We and Where Are We Going.' A look at HIPAA just before the deadline for the implementation of the first of the HIPAA regulations. The date is March 17**. Details in upcoming issues.
Expert Q&A HIPAA: Where are we, and where are we going?
Looking backwards, we are six years into the process of converting an Act of Congress -- the Health Insurance Portability and Protection Act -- into regulations and real world solutions. Looking forward, we are weeks away from the deadline to meet the Privacy regulations and roughly seven months away from the deadline for Transactions and from the deadline for Security. Hal Amens, editor of the HIPAA Implementation Newsletter, will tell you what you still need to do to reach these deadlines.
Ask Hal your questions now
mailto:editor@searchsecurity.com?subject=HIPAA-THIN
Sixth National HIPAA Summit Features Leading Healthcare Privacy & HIPAA Regulators -- March 26-28, 2003; Washington DC. For registration Information call 800-684-4549 or email: registrationhq@aol.com. You may register with secure online registration and additional information at http://www.hipaasummit.com

---

management consultants and sources we consider reliable. There are no further warranties about accuracy or applicability. It contains neither legal nor financial advice. For that, consult appropriate professionals. Lyon, Popanz & Forester http://lpf.com is a management consulting firm that designs and manages projects that solve management problems. Planning and project management for HIPAA are areas of special interest.